


THE **WORLD'S** **LARGEST** **BOOK** **STORES**


Richard P. Berg

Enclosure: Appendix A (4 pages)

Appendix A

(VERSION WITH MARKINGS TO SHOW CHANGES MADE)

Page 1 of 4

1. (Amended) Computing apparatus comprising mounted on an assembly main processing means [and] main memory means and a trusted device, each being connected for communication with one or more other components on the assembly,
[characterised by further comprising a trusted device mounted on the assembly and being connected for communications with one or more other components on the assembly,] the trusted device being arranged to acquire a true value of an integrity metric of the computing apparatus.
4. (Amended) Computing apparatus according to claim 3, wherein the [platform] computing apparatus is arranged to cause the instructions to be the first instructions executed after release from reset.
5. (Amended) Computing apparatus according to claim 3 [or claim 4], wherein the trusted device is arranged to transfer the instructions to the main processing means in response to memory read signals from the main processing means.
6. (Amended) Computing apparatus according to [any one of claims 1 to 5] claim 1, wherein the trusted device comprises device memory means and is arranged to monitor [the] a data bus means by which components mounted on the assembly are adapted to communicate and store in the device memory means a flag in the event the first memory read signals generated by the main processing means after the computing apparatus is released from reset are addressed to the trusted device.

(VERSION WITH MARKINGS TO SHOW CHANGES MADE)

Page 2 of 4

7. (Amended) Computing apparatus according to [any one of claims 1 to 6]claim 1, wherein the trusted device has stored in device memory means at least one of:

a unique identity of the trusted device;

an authenticated integrity metric generated by a trusted party; and

a secret.

10. (Amended) Computing apparatus according to claim 8 [or claim 9], wherein the trusted device has stored in device memory means an authenticated integrity metric generated by a trusted party and includes a encryption function, the trusted device being arranged to generate a response to a received challenge, the response comprising an acquired integrity metric and the authenticated integrity metric, both signed by the encryption function using the private asymmetric encryption key.

Please cancel claim 11 without prejudice.

(VERSION WITH MARKINGS TO SHOW CHANGES MADE)

Page 3 of 4

12. (Amended) A method of operating a system comprising a trusted computing apparatus and a user, the trusted computing apparatus incorporating a trusted device being arranged to acquire the true value of an integrity metric of the trusted computing apparatus, the method comprising the steps of:

the trusted device acquiring the true value of the integrity metric of the trusted computing apparatus;

the user generating a challenge for the trusted computing apparatus to prove its integrity and submitting the challenge to the trusted computing apparatus;

the trusted computing apparatus receiving the challenge, and the trusted device generating a response including the integrity metric and returning the response to the user; and

the user receiving the response, extracting the integrity metric from the response and comparing the integrity metric with an authenticated metric for the trusted computing apparatus that had been generated by a trusted party.

16. (Amended) A method of establishing a communications channel in a system between trusted computing apparatus and remote computing apparatus, the method including the step of the remote computing apparatus verifying the integrity of the trusted computing apparatus using the method according to [any one of claims 12 to 15]claim 12, and maintaining the communications channel for further transactions in the event the integrity of the trusted computing apparatus is successfully verified by the remote computing apparatus.

